FLA-IoT: Virtualization Enabled Architecture for Heterogeneous Systems in Internet of Things

Irfan Latif Memon[1]

Department of Electrical Engineering
Sukkur IBA University
Airport Road, Postal Code 65200, Sukkur, Pakistan

Shakila Memon[2]

Department of Electronics
Mehran University of Engineering and Technology
Jamshoro, Sindh

Junaid Ahmed Bhatti[3], Abdul Sattar Chan[5]

Department of Electrical Engineering
Airport Road Postal Code 65200
Sukkur Pakistan

Raheel Ahmed Memon[4]

Department of Computer Science
Sukkur IBA University, Airport Road
Postal Code 65200, Sukkur, Pakistan

Abstract—**A flexible architecture is always required when trying to communicate with heterogeneous kind of systems, and IoT is the largest communication network of the history, which is bringing life to everything around us. Currently available three and four layered communication architectures are the popular basic structures to implement IoT. Where three Layers architecture is composed of perception, network and application layers and four layer architecture is composed of perception, network, service, application layer. The problem with existing architectures is that some layers are not well managed and complex in structure and lacks in the interoperability of different kind devices. In this research we present a virtualization enabled architecture Flexible Layered Architecture for Internet of Things (FLA-IoT) to overcome those challenges. FLA-IoT provides a simple structure with well-organized layers and introduces the creation of Virtual Mote (virtual object) from all real-world devices to enable the communication between unlike devices. This results in an indiscriminate communication between different real-world devices with a well-managed layered architecture.**

Keywords—Internet of Things; virtualization; virtual mote; cloud; heterogeneous systems

I. INTRODUCTION

Currently, we are dealing with a number of Internet-enabled devices, which can be brought into broad categories like Computers, Mobile Phones, Embedded Devices and Industrial equipment. The upcoming trend of Communication will expand the range and within a few years a huge number of new categories will be introduced, we can say that; Electricity distribution systems, Interior fixtures and holdings, vehicles, residential and commercial buildings, animals, home appliances, personal care accessories, and groceries could be only a few objects using upcoming communication technologies[1]. The era where all the objects around us will be communicating with each other is known as Internet of Things (IoT) also known as Cyber-Physical Systems (CPS). It is also referred as Internet of everything or Internet of Infinite things. As this field has different names, it also has several definitions and several theoretical assumptions at the same time. Some forms of IoT has implemented so far by

embedding sensing and actuation in different devices. For example, buildings in these days are already equipped with sensing technologies to control lights, security, and temperature of the environment. As another example, for safety on roads, several improvements have been done so far, like controlling traffic intelligently by using, real-time decisions systems. The vehicles are embedded with sensors. Industrial equipment, health care services, smart mobile phones etc., can be counted as a part of today's IoT. However, all these developments are just tip of the iceberg. We can say at this time we are still in the immature phase of developments of upcoming technology [2], [3].

IoT will be a completely new generation and a new concept of Internet technology, which would be dealing massively large networks of heterogeneous systems. This much large and heterogeneous network has a lot of challenges and milestones to achieve [4]. The most common challenges that have been identified are: Detection and Identification of devices, standard architecture of network, various communication technologies, basic set of protocols, grouping and forming networks in real time, management technologies, big data and signal processing, efficient search engines, storage, power, security, standardization and hardware developments[5]–[8].

According to Gartner hype cycle of 2012[9], 2013[10], 2014[11] and 2015[12] shown in Fig. 1, Internet of things is maintaining itself on the hype of the curve. Fig. 2 evidence that IoT is growing every year and giving birth to several new fields and influencing the stable technologies; Gartner Hype Cycle of 2016 and 2017 shows the emerging trends of IoT Technology (such as Smart Workspace, Connected homes, Autonomous Vehicles, Blockchain, IoT platform) [13]. According to the Gartner Hype Cycle of 2019 shown in Fig. 3 that, Internet of Things gave birth to several new field such as Digital Business Technology Platform, Digital Twin, IoT Security, IoT Services, Indoor Location for People, Edge Analysis [14]. However, this could be considered only the start, it's possible that tomorrow IoT field would give birth to several new fields and Gartner would be showing only

different fields of IoT on its overall hype cycle [15][16]. It's a fact that IoT is tomorrow's technology which will replace every development contradicting to this.

The evolution and adoption of digital infrastructure is five times faster than that of electricity and telephony. By 2020 it is expected that there would be 37 billion connected devices around the world [17]. Thus there is a need of an architecture which should be very much flexible to sustain the evolution of upcoming era of the internet. Setting up the platform of communication of these billions of devices is still a challenge. Many developments have been done so far. There are two kinds of architectures very much prominent in the field of IoT 3 Layer IoT architecture and 4 Layer Service Oriented Architecture. Several executions are made on the basis of these two architectures. But there are several problems with the existing architectures:

Simplicity: Architecture is needed which should be very simple and straightforward in its implementation.

Organization: Well organized and well-managed architecture, so that each layer of proposed architecture should be entitled to perform related tasks.

Interoperability: An architecture that should be able to operate in heterogeneous kind of environment. So that things can communicate easily even if underlying hardware varies from every expects of real life.
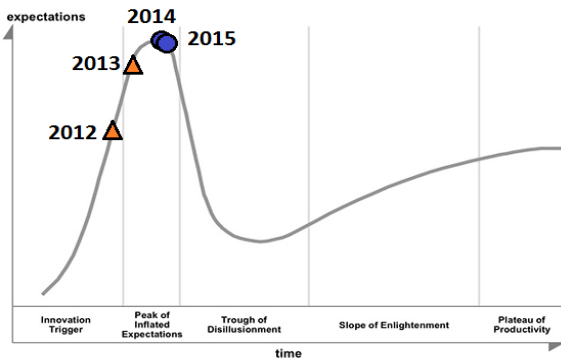

Fig. 1.   Gartner Hype Cycle of Last Four Years Showing Embryonic Phase of IoT.
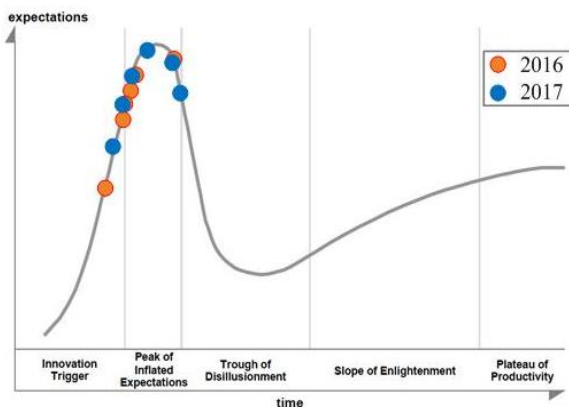

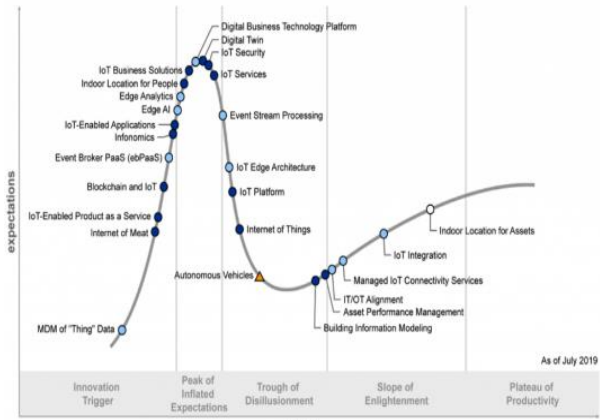Fig. 2.   Gartner Hype Cycle of 2016 and 2017 Emerging Phase of IoT.

Fig. 3.   Gartner Hype Cycle of 2019 for Trends of Internet of Things.

In this research work an architecture named as Flexible Layered Architecture for the Internet of Things (FLA-IoT) is proposed, it is a five-layer architecture (Perception Layer, Network Layer, Virtualization Layer, Service Layer and Application Layer) The Virtualization and Service Layer resides in the FLA-IoT Cloud. The proposed architecture is an effort to provide the clear definition to the operating elements and functions of IoT.

The three-layer architecture which is composed of Perception Layer, Network Layer, and Application Layer, has very complex structure because of various different type of responsibilities on Network and Application layers, in response to that 4 layer architecture has been proposed, which has added an additional Service Layer in between Network and Application layer to reduce the burden of the two layers. But still the interoperability has not dealt in the 4 layer architecture, and also service layer is still not solely dedicated to providing the services only.

The proposed architecture further simplifies and organizes the elements and functions of IoT on its layered structure.

The proposed architecture come up with an additional layer named as virtualization layer in between the service and network layers.

A platform for heterogeneous systems to communicate flexibly with almost any device belongs to different categories, hardware structure, platform operations and a different set of protocols.

Rest of the paper is organized as, section two provides literature survey, Section 3 is about proposed virtualization enabled architecture with a detailed discussion on working of each component. Section four provides experimental results before concluding in section five.

II.   Literature Survey

The field of IoT has come up with a lot of contributions from different computer scientists and researchers addressing several different issues related that field. Generally, the IoT architecture is divided into two different kinds of architectures. The first one is 3 Layer Architecture, and the second one is 4 Layer Architecture. The three-layer

architecture has perception layer, network layer and application layer which also serve as business and service layer. And the second one is 4 layer architecture, which has an additional service layer at the bottom there is perception layer, then network layer, service layer and at the top, there is an application layer.

In three-layer architecture, physical layer performs the task of sensing the objects of the real world, network layer performs routing and transmission tasks and additional it is also responsible for data services like data aggregation and data computing. Application layer performs business analysis, services management, composition related tasks and the interfacing to interact with machines and humans.

The three-layer architecture has become very popular architecture and several works have been done to improve the flexibility of IoT and to maximize utilization of existing resources using it. One of such work done in [18] focusing on utilizing the existing wireless sensor network in a building at Parvoda University in Italy. This is done via shared standards working with protocols such as 6LowPAN. Another work was done by Van de Abeele proposed a reference model, which performed on the behalf of devices by intercepting all the requests, transforming to and from Constrained Application Protocol (CoAP) [19].

Simone Cirani et al. [20] proposed a scalable and self-configuring peer-to-peer (P2P)-based architecture for large-scale IoT networks, intended to provide automated service and resource discovery mechanism without human interactions.

IoT and Cloud Convergence is another work done in the year 2013 by Suciu, George, et al. [21]. It focuses to combine another research area to IoT by involving Cloud Computing. It suggests that the sensors and actuators should be hosted in a cloud to enable interoperability among the main complementary technologies and named it as Cloud of Things.

There are several other interesting models proposed in [22]–[25], which are mainly focusing on three-layered architecture, such as Sensing Layer, Network Layer, Service or Application Layer as shown in Fig. 4.

The 3 Layer architecture is a multilayer architecture of IoT, but from function and operation point of view, the network and application layers are complex, because the network layer doesn't only perform routing and transmission tasks but also responsible to provide data services like data aggregation and computation. Similarly, the application layer besides performing its basic task of providing services to different kind of devices and customer quires, it is also additionally responsible for some extra tasks like data mining and data analysis [26].

For performing explicitly only service related tasks, Service-Oriented Architecture has been proposed, which deals with data service issues like; data aggregation, computation, data mining, data analytics etc, the SoA based IoT Architecture added a new layer named as Service Layer in between application and network layer [27]–[29]. Ideally, this layer extract the data service tasks which were traditionally performed by the application and network layers will be now hosted and dealt at Service layer. As shown in Fig. 5, the Service Oriented Architecture has four layers, Sensing Layer, Network Layer, Service Layer and Application Layer. Where the additional service layer is further divided into three sub-layers (Composition, management, and the business) to perform tasks of discovering desired service requests, to interact with connected objects composition service is used, for interacting and managing the service requests efficiently management service is used, and service interfacing to application layer [26].

These architectures are good in a way that they resolved basic communication problems efficiently and provided a structure for that. The thing observed in literature is that somehow interaction between the heterogeneous devices is taken very lightly. While the interoperability is equally important as security and other issues are. Our proposed architecture bring up a new high level layered architecture which is a modification of existing 4 layers SoA based architecture by adding up a new Virtualization layer. Thus its 5 layer architecture and the layers are Perception Layer (same as Sensing Layer), Network Layer, Virtualization Layer, Service Layer and Application Layer. The architecture is named as Flexible Layered Architecture for Internet of Things (FLA-IoT). In the proposed architecture, Virtualization layer creates a logically friendly environment by creating virtual objects of real-world sensing devices, which is known as Virtual Mote, so that each and every device despite its size, architecture, operating system and type of data could communicate with each without any hindrance. FLA-IoT considers well-known protocols for implementation.
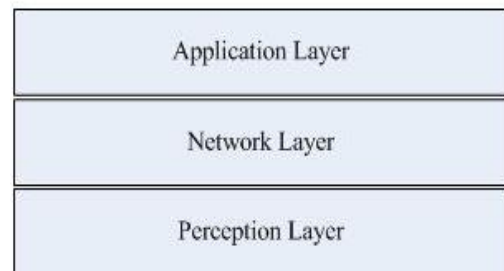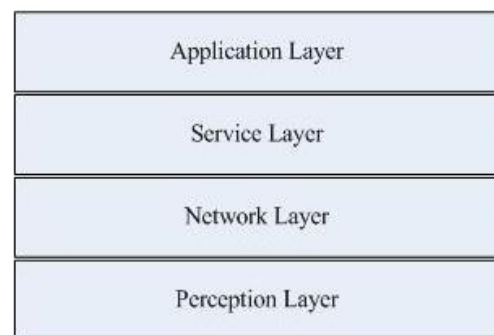

Fig. 4.   Three Layer Architecture.

Fig. 5.   Service Oriented Architecture for IoT.

III. PROPOSED FLEXIBLE LAYERED ARCHITECTURE

The Internet model considered to be modified to accommodate the new generation of internet and its advanced technologies. In this, I propose an architecture, which is simple in its implementation, well organized from its functional point of view and flexible to adopt any kind of technology, at the same time it maintains security and manages the resources equally. The proposed architecture is on based on virtualization and named as Flexible Layered Architecture of Internet of Things (FLA-IoT). The FLA-IoT has five Layers from which two layers resides in the FLA-IoT Cloud. As shown in Fig. 6, the Layers of architecture starting from the bottom are; Perception Layer, Network Layer, Virtualization and Service Layer (Both resides in FLA-IoT Cloud), and then at the top there is Application Layer.

The Perception, Network and Application layers work on the same philosophy as of four layers architecture, but the Virtualization Layer and Service Layer brings up the difference by introducing simplicity, organization, and heterogeneity.

A. Perception Layer

This layer is responsible for perceiving and reacting, it is also known as sensing layer. The perception the layer is implemented as a bottom layer where it interacts with several real-world devices or things. The perception task can be done using different kinds of RFID tags, sensors, actuators, etc. to observe the surrounding environment. Its main objective is to generate data from living/nonliving objects of real world and bring them into the category of things that can speak.
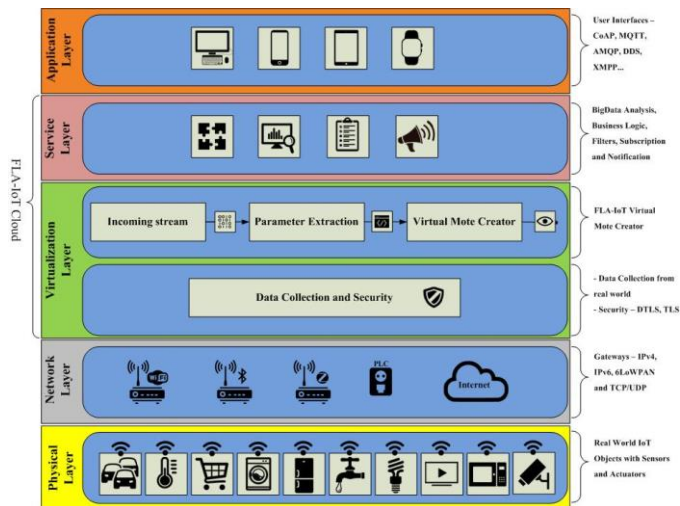

Fig. 6. Flexible Layered Architecture of IoT.

B. Network Layer

Network Layer also knew as transmission layer, the Network layer is responsible for the exchange of perceived data or commands in between FLA-IoT Cloud and the installed devices to receive and react in particular situations. On this layer, the potential communication technologies are ZigBee, Wifi, Bluetooth, Powerline Communication (PLC) and the Internet (3G, 4G/LTE/LTE-A, Ethernet) through this layer the data is passed to FLA-IoT Cloud. The

communication is achieved by protocols like IPv4/IPv6, 6LoWPAN, TCP/UDP to enable the talk between of different kind of devices and FLA-IoT Cloud.

C. Virtualization Layer

The FLA-IoT Cloud is composed of two layers one is Virtualization Layer and the other one is Service Layer, Fig. 6 shows the detailed view of both Layer. This additional Virtualization layer works as a bridge between the real and cyber world, it extends the scope of IoT to make it more flexible and scalable to all type of interactions from heterogeneous devices by creating their virtual objects of real-world devices, which is known as a Virtual Mote (VM).

VMs are used to perform several existing and new tasks to satisfy the service needs initiated by the end users and administrators. The benefit of creating a VM that different object can communicate with each other by using virtual objects, for example washing machine at your home can communicate with grid station using smart meters to find out the suitable time when the price of a unit is pretty down to start the pending washing tasks. Though the architecture of underlying hardware is different, the communication could be established easily. In the creation of Virtual Mote, there are six steps involved as shown in Fig. 7. Further Fig. 8 shows the flow of a process performed by Virtualization Layer, for creating virtual mote and adding/updating existing data on sensor log server.

1) Data collection: It is responsible for collecting data from different resources of environments by using thousands of different sensors.

2) Security: Security is important to consider because in IoT it is a common vulnerable when the data is exchanged between user and devices[30]. For example, a toaster and oven could get the virus to burn the food items or, the severe attacks to take the control of traffic signals, unauthorized access of secret information, and disrupt critical services are only a few examples of attacks in IoT. For the security, we consider well-known protocols: Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) for TCP and UDP transport. The reason to choose these protocols is that IoT communities like IETF and oneM2M have already started working on DTLS and has strongly initiated to standardize the DTLS for IoT security, some other groups are also working on optimization and support of DTLS and other IoT protocols in constrained environment (such as constrained devices and networks) [30], [31].

3) Parameter extraction: the parameter extraction is performed using popular metadata formats JavaScript Object (JSON) and Extensible Markup Language (XML).

4) Sorting: After Passing the security and parameter extraction phases of FLA-IoT, the stream of incoming data is received and sorted into the categories and location wise on the basis of device ID, device type, and device location.

5) Virtual mote: As shown in Fig. 8, The Virtual Mote creation checks whether the incoming stream has already an object created or not, if the same id device has an object created then that object would be retrieved and the new

readings would be updated on sensor log server (which is meant to keep the history for data analytics task on service layer). If the object is not already created for that device then the new object is created and assigned the first values as received. The data on Sensor Log Server will be used by service layer for applying business logic and big data analytics to response the queries from different users and machines.

6) New entry or updates existing: If the object already exists here, the new readings from the real world be updated on to Sensor Log Server, otherwise Virtual Mote Creation would take place and in this phase, the new entry would be created in databases for the new incoming data stream.

D. Service Layer

This is the second layer in FLA-IoT Cloud and the fourth layer in FLA-IoT architecture, it performs three main tasks: Maintains Sensor Log, Apply Business Logics, and deal with Interactions like; request/response and publish/subscribe models; as shown in Fig. 7. The Sensor log Server is responsible to hold the historical data of each device, which is used for analysis by the Business logic server, and the Interaction Server is used to notify the specific information to are lated person, machine or response the commands to react in particular situations. For example, in the situation of Fire in the building, it sends the notification to local fire brigade office and maybe trigger fire sprinkler systems to rescue.

E. Application Layer

This layer is intended for user end, either intercepted by human or other machines, but it enables the information exchange between the devices and user end.

The set of protocols operates on this layer are Constrained Application Protocol (CoAP), Data Distribution Service (DDS), MQ Telemetry Transport (MQTT) and Extensible Messaging and Presence Protocol (XMPP).

For the application layer protocols different development groups and standardization bodies have taken the initiatives to declare the required communication protocols. Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), European Telecommunications Standards Institute (ETSI), Object Management Group (OMG), Advanced Open Standards for the information society (OASIS), Joint Technical Committee (JTC) of International Standardization Organization (ISO) and International Electrotechnical Commission (IEC) are the most prominent

standardization bodies actively participating in the development of the IoT protocols (specifically application layer). Table I describes the protocols on application layer in further detail.
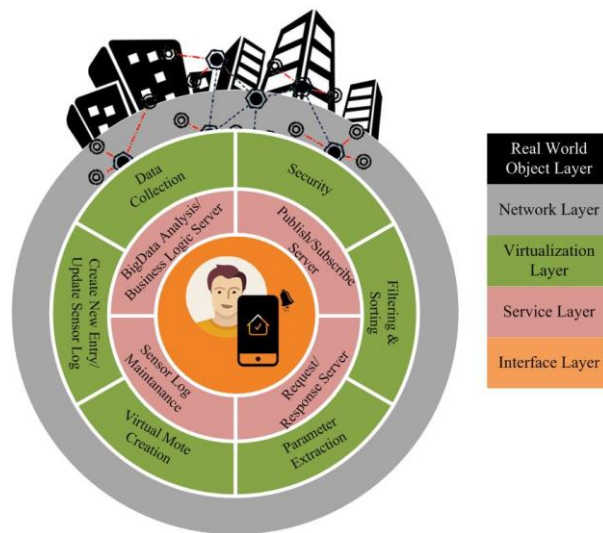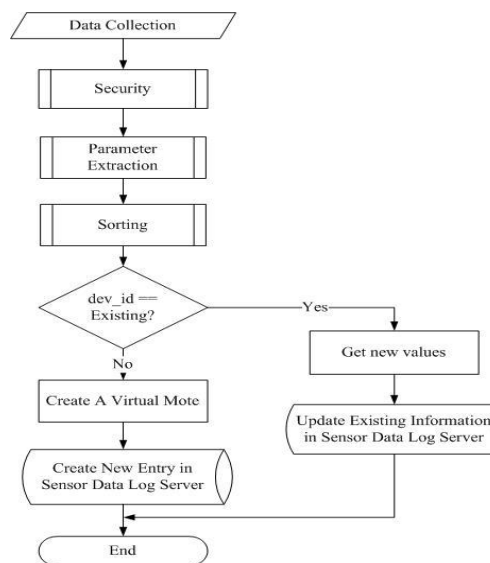

Fig. 7. Standard FLA-IoT Workflow.

Fig. 8. Virtualization Layer Underlying Process.

TABLE I.   PROTOCOLS ON APPLICATION LAYER AND THEIR WORKING

Protocol	Standardization	Model	Transport Protocols	Architecture	Short Working Description
CoAP	IETF	Request/Response Publish/Subscribe	UDP	Centralized	non-conformable, acknowledgment, reset, piggybacked, separate response and empty messages
DDS	OMG	Publish/Subscribe	TCP	Decentralized	Supports 23 QoS policies which cover wide variety of communication uses cases which provides better reliability and QoS, for example, security, priority and reliability
MQTT	OASIS	Publish/Subscribe	TCP	Centralized	Three options to achieve QoS:On Delivery (at Most), On Delivery (at least), On Delivery (exactly),
AMQP	ISO/IEC	Publish/Subscribe	TCP	Centralized	Used in business and commercial platforms, it is scalable and supports heterogeneous and interoperable communication among different devices and different languages.
XMPP	IETF	Request/Response Publish/Subscribe	TCP	Decentralized	Multidirectional Communication (push and pull data)

IV. RESULTS

To validate our proposed system we choose a controlled environment of a cold storage for food items. Usually in a cold storage there are multiple sensors installed at several locations. Instead of installing the sensors at each location of cold storage, we use a patrolling drone planted with a temperature sensor to monitor multiple locations of entire silo. The drone is moved around different locations for obtaining readings at different time interval for maintaining the internal temperature in between 18 and 22 Celsius. Whereas, each location is virtually stored as a virtual mote (VMT) sensor in cloud datacenter.

Fig. 9 shows the obtained readings at different time intervals for different locations, where the cloud organize the readings as virtual motes VMT1 through VMT5.

The JSON format data is shown in Fig. 10 which is being collected using patrolling drone around the multiple locations of cold storage. It can be seen that every time drone moves to a new location L1 to L5, it shows the collected data as a reading from different sensors instead of different locations.
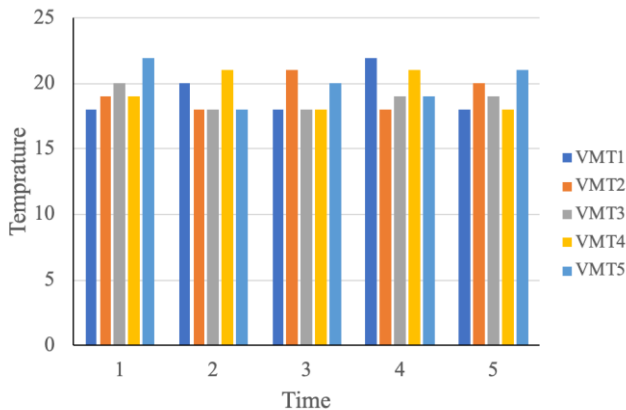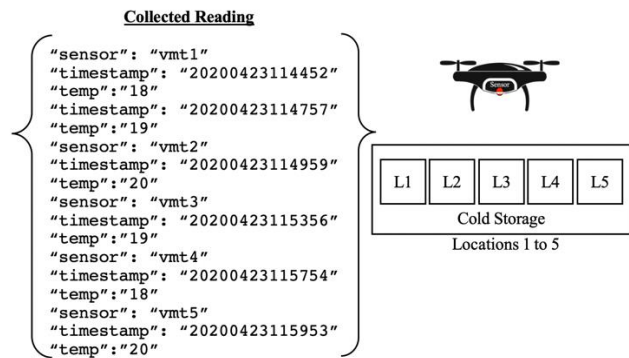
Fig. 9.   Virtual Mote Sensor Readings.

Collected Reading

"sensor": "vmt1"
"timestamp": "20200423114452"
"temp":"18"
"timestamp": "20200423114757"
"temp":"19"
"sensor": "vmt2"
"timestamp": "20200423114959"
"temp":"20"
"sensor": "vmt3"
"timestamp": "20200423115356"
"temp":"19"
"sensor": "vmt4"
"timestamp": "20200423115754"
"temp":"18"
"sensor": "vmt5"
"timestamp": "20200423115953"
"temp":"20"

Fig. 10. Collected JSON Format Data From Multiple Locations.

V. CONCLUSION

This world is trying hard to become instrumented, interconnected and intelligent, and IoT is the only solution to that effort; however, the challenge is to facilitate the communication of huge network of heterogeneous types of systems. To overcome that challenge, the basic building blocks are required to be standardized and the basic building blocks are communication architecture, a basic set of protocols, security, and resource management. In this work, we propose a 5 layered architecture named as Flexible Layered Architecture for Internet of Things (FLA-IoT), which comes up to resolve the problems of simplicity, organization, and interoperability in existing 3 and 4 layered architectures of IoT. The FLA-IoT is a virtualization enabled cloud-based architecture and introduces the Virtual Mote (VM) so that real life objects can communicate seamlessly. The overall construction of 5 Layered architecture is as: at the bottom there is a perception layer deals with sensing real-world environment by using tags, sensors, and actuators, then there is network layer, responsible for communication between FLA-IoT Cloud and real world, the proposed virtualization layer which resides in the FLA-IoT Cloud, it deals with the security of the incoming/outgoing data streams, and virtual mote creation, which enable the communication between heterogeneous kind of system. Then we have service layer it also resides in the FLA-IoT Cloud and deals with the business logic, big data analytics and interactions like publish/subscribe or request-response modes. Finally, the application layer,

which runs several kind APIs to interact with the real-life objects. To validate the proposed system an experiment is conducted for cold storages for provisioning the sensors as virtual motes in an IoT enabled environment. The results shows that the proposed FLA-IoT can be applied to any type of device or system for creating its virtual instance.

REFERENCES

[1] R. Memon, J. Li, J. Ahmed, M. Nazeer, M. I. I. T., and undefined 2019, "Cloud-based vs. blockchain-based IoT: A comparative survey and way forward," Springer.

[2] Y. Kumar, R. B.-P. Technology, and undefined 2015, "Key aspects of smart grid design for distribution system automation: Architecture and responsibilities," Elsevier.

[3] F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," Business and Information Systems Engineering, vol. 57, no. 3. Gabler Verlag, pp. 221–224, 01-Jun-2015, doi: 10.1007/s12599-015-0383-3.

[4] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities," Futur. Internet, vol. 12, no. 4, p. 61, 2020, doi: 10.3390/fi12040061.

[5] A. Whitmore, A. Agarwal, L. D. X.-I. S. Frontiers, and undefined 2015, "The Internet of Things—A survey of topics and trends," Springer.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[7] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," IEEE Commun. Mag., vol. 50, no. 6, pp. 134–143, 2012, doi: 10.1109/MCOM.2012.6211498.

[8] O. Monnier, "Introduction," Texas Instruments, pp. 1–11, 2013.

[9] "Hype Cycle for Emerging Technologies, 2012," 2012. [Online]. Available: https://www.gartner.com/en/documents/2100915/hype-cycle-for-emerging-technologies-2012. [Accessed: 17-Mar-2020].

[10] "Hype Cycle for Emerging Technologies, 2013," 2013. [Online]. Available: https://www.gartner.com/en/documents/2571624/hype-cycle-for-emerging-technologies-2013. [Accessed: 17-Mar-2020].

[11] "Hype Cycle for Emerging Technologies, 2014," 2014. [Online]. Available: https://www.gartner.com/en/documents/2809728/hype-cycle-for-emerging-technologies-2014. [Accessed: 17-Mar-2020].

[12] "Hype Cycle for Emerging Technologies, 2015," 2015. [Online]. Available: https://www.gartner.com/en/documents/3100227/hype-cycle-for-emerging-technologies-2015. [Accessed: 17-Mar-2020].

[13] "Hype Cycle for the Internet of Things, 2017." [Online]. Available: https://www.gartner.com/en/documents/3770369/hype-cycle-for-the-internet-of-things-2017. [Accessed: 17-Mar-2020].

[14] "Hype Cycle for the Internet of Things, 2019." [Online]. Available: https://www.gartner.com/en/documents/3947474/hype-cycle-for-the-internet-of-things-2019. [Accessed: 17-Mar-2020].

[15] "'Internet of Meat' is on the rise, says Gartner - Which-50." [Online]. Available: https://which-50.com/internet-of-meat-is-on-the-rise-says-gartner/. [Accessed: 17-Mar-2020].

[16] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "DualFog-IoT: Additional fog layer for solving blockchain integration problem in internet of things," IEEE Access, vol. 7, pp. 169073–169093, 2019, doi: 10.1109/ACCESS.2019.2952472.

[17] Cisco Systems Inc., "The Internet of Things Reference Model," in Internet of Things World Forum, 2014, pp. 1–12.

[18] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, and M. Zorzi, "Architecture and protocols for the internet of things: A case study," in 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2010, 2010, pp. 678–683, doi: 10.1109/PERCOMW.2010.5470520.

[19] F. Van Den Abeele, J. Hoebeke, I. Moerman, and P. Demeester, "Fine-grained management of CoAP interactions with constrained IoT devices," in IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World, 2014, doi: 10.1109/NOMS.2014.6838368.

[20] S. Cirani et al., "A scalable and self-configuring architecture for service discovery in the internet of things," IEEE Internet Things J., vol. 1, no. 5, pp. 508–521, 2014, doi: 10.1109/JIOT.2014.2358296.

[21] G. Suciu, S. Halunga, A. Vulpe, and V. Suciu, "Generic platform for IoT and cloud computing interoperability study," in ISSCS 2013 - International Symposium on Signals, Circuits and Systems, 2013, doi: 10.1109/ISSCS.2013.6651222.

[22] J. Li, E. Altman, and C. Touati, "A General SDN-based IoT Framework with NVF Implementation," ZTE Commun., vol. 13, no. 3, pp. 42–45, 2015.

[23] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[24] P. Fremantle, "A Reference Architecture for the Internet of Things."

[25] M. Bauer et al., "Introduction to the architectural reference model for the internet of things," Internet-of-Things Archit. IoT-A Deliv. D1. 3 Updat. Ref. Model IoT v1, vol. 5, 2012.

[26] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.

[27] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[28] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in Proceedings - International Conference on Distributed Computing Systems, 2008, pp. 495–500, doi: 10.1109/ICDCS.Workshops.2008.40.

[29] G. Gan, Z. Lu, J. J.-2011 international conference on Internet, and U. 2011, "Internet of things security analysis," 2011 Int. Conf. internet Technol. Appl., pp. 1–4, 2011.

[30] H. Tschofenig and T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things," IETF, pp. 1–61, 2016.

[31] R. T. Tiburski, L. A. Amaral, E. De Matos, D. F. G. De Azevedo, and F. Hessel, "The Role of Lightweight Approaches Towards the Standardization of a Security Architecture for IoT Middleware Systems," IEEE Commun. Mag., vol. 54, no. 11, pp. 56–62, 2016, doi: 10.1109/MCOM.2016.1600462CM.